

100

2. The identification system of claim 1, wherein each of said end terminals is configured to cipher the biometrics data so that the biometrics data contained in said transaction request message and said authentication request message is the ciphered biometrics data, and wherein said authentication server is configured to decipher the ciphered biometrics data

6 contained in the received authentication request message.

1           3.     The identification system of claim 1, wherein said ECSP unit  
2 includes a conversion table for mapping a first plurality of user identifiers to  
3 a second plurality of user identifiers, wherein said first plurality of user  
4 identifiers are used by said plurality of end terminals and said second  
5 plurality of user identifiers are the user identifiers registered in said database,  
6 said ECSP unit converting the user identifier contained in the received  
7 transaction request message to one of the second plurality of user identifiers  
8 which is mapped to the received user identifier and transmitting said  
9 authentication request message containing the converted user identifier.

1           4.     The identification system of claim 1, wherein each of said end  
2 terminals is configured to cipher the biometrics data with a secret key  
3 generated by a variable secret key generator which generates secret keys  
4 which vary with time, the generated secret key being agreed-upon with said  
5 authentication server.

1           5.     The identification system of claim 4, wherein said variable  
2 secret key generator is located at said authentication server and wherein each  
3 of said end terminals is configured to transmit a key request message to said  
4 authentication server via said ECSP unit to receive said secret key from the  
5 secret key generator and ciphering the biometrics data with the received  
6 secret key before said transaction request message is transmitted.

1           6.     The identification system of claim 5, wherein said  
2 authentication server comprises a variable secret key generator which  
3 generates a secret key which varies with time , and a decryption unit for  
4 deciphering the received ciphered biometrics data by using the secret key  
5 generated by said secret key generator.

1           7.     The identification system of claim 1, wherein each of said end  
2 terminals comprises a user terminal exclusively owned by said user.

1           8.     The identification system of claim 1, wherein each of said end  
2 terminals comprises a sales terminal to which a plurality of user's handheld  
3 personal units can be connected, wherein said sales terminal transparently  
4 transmits a transaction request messaged received from each of the personal  
5 units to said ECSP unit.

1           9.     The identification system of claim 1, wherein said biometrics  
2 data of said user is a fingerprint of said user.

1           10.    The identification system of claim 1, wherein said biometrics  
2 data of said user is an extracted feature of a fingerprint of said user.

1           11.    An identification system comprising:  
2           a plurality of end terminals respectively identified by user identifiers,  
3 each of the end terminals transmitting a transaction request message  
4 containing biometrics data of a user to a communications network;

5 at least one electronic commerce service provider (ECSP) unit for  
6 receiving said transaction request message via said network and transmitting  
7 an authentication request message containing said biometrics data to said  
8 network; and

9 an authentication server having a database for mapping a plurality of  
10 registered biometrics data to a plurality of corresponding registered user  
11 identifiers, the authentication server receiving the authentication request  
12 message via said network, comparing the received biometrics data to all of  
13 the registered biometrics data in said database, detecting the user identifier  
14 mapped to the biometrics data which coincides with the received biometrics  
15 data, and returning a reply to said ECSP unit via said network indicating that  
16 a user identified by the detected user identifier is authenticated.

1 12. The identification system of claim 11, wherein each of said end  
2 terminals is configured to cipher the biometrics data so that the biometrics  
3 data contained in said transaction request message and said authentication  
4 request message is the ciphered biometrics data, and wherein said  
5 authentication server is configured to decipher the ciphered biometrics data  
6 contained in the received authentication request message.

1 13. The identification system of claim 12, wherein each of said end  
2 terminals is configured to cipher the biometrics data with a secret key  
3 generated by a variable secret key generator which generates secret keys  
4 which vary with time, the generated secret key being agreed-upon with said  
5 authentication server.

1           14.    The identification system of claim 13, wherein said variable  
2   secret key generator is located at said authentication server and wherein each  
3   of said end terminals is configured to transmit a key request message to said  
4   authentication server via said ECSP unit to receive said secret key from the  
5   secret key generator and ciphering the biometrics data with the received  
6   secret key before said transaction request message is transmitted.

1           15.    The identification system of claim 14, wherein said  
2   authentication server comprises a variable secret key generator which  
3   generates a secret key which varies with time, and a decryption unit for  
4   deciphering the received ciphered biometrics data by using the secret key  
5   generated by said variable secret key generator.

1           16.    The identification system of claim 12, wherein each of said end  
2   terminals comprises a user terminal exclusively owned by said user.

1           17.    The identification system of claim 12, wherein each of said end  
2   terminals comprises a sales terminal to which a plurality of user's handheld  
3   personal units can be connected, wherein said sales terminal transparently  
4   transmits a transaction request message received from each of the personal  
5   units to said ECSP unit.

1           18.    The identification system of claim 12, wherein said biometrics  
2   data of said user is a fingerprint of said user.

1           19.    The identification system of claim 12, wherein said biometrics  
2   data of said user is an extracted feature of a fingerprint of said user.

1           20.    An identification method comprising the steps of:

- 2           a)    transmitting, from an end terminal, a transaction request  
3   message containing biometrics data of a user to a communications network;  
4           b)    receiving, at an electronic commerce service provider, said  
5   transaction request message via said network;  
6           c)    transmitting, from the electronic commerce service provider, an  
7   authentication request message containing said biometrics data to said  
8   network;  
9           d)    receiving said authentication request message via said network  
10   at a user authenticator having a database for storing a plurality of registered  
11   biometrics data;  
12           e)    determining whether the received biometrics data has  
13   corresponding biometrics data in said database; and  
14           f)    returning a reply from said user authenticator to said electronic  
15   commerce service provider via said network indicating that said transaction  
16   request message is authenticated if the received biometrics data coincides  
17   with one of the registered biometrics data of the database.

1           21.    The identification method of claim 20, wherein the step (a)  
2   further comprises ciphering the biometrics data and transmitting said  
3   transaction request message containing the ciphered biometrics data to said  
4   network, and wherein the step (d) further comprises the step of deciphering

5 the biometrics data contained in the received authentication request message.

1 22. An identification method comprising the steps of:

2 a) transmitting, from an end terminal, a transaction request  
3 message containing biometrics data of a user and a user identifier of said user  
4 to a communications network;

5 b) receiving, at an electronic commerce service provider, said  
6 transaction request message via said network;

7 c) transmitting, from the electronic commerce service provider, an  
8 authentication request message containing said biometrics data and said user  
9 identifier to said network;

10 d) receiving said authentication request message at a user  
11 authenticator via said network, the authenticator having a database in which  
12 a plurality of registered biometrics data are mapped to a plurality of  
13 corresponding registered user identifiers;

14 e) comparing the received biometrics data to one of the registered  
15 biometrics data which is mapped in said database to the user identifier  
16 contained in said authentication request message; and

17 f) returning, from the user authenticator, a reply to said electronic  
18 commerce service provider via said network indicating that said transaction  
19 request message is authenticated if the received biometrics data coincides  
20 with said mapped biometrics data.

1 23. The identification method of claim 22, wherein the user  
2 identifiers stored in said database are different from the user identifiers of

3 said end terminals, further comprising converting, at said service provider,  
4 the user identifier contained in the received transaction request message to a  
5 second user identifier which is contained in said authentication request  
6 message as the first-mentioned user identifier.

1 24. The identification method of claim 22, wherein the step (a)  
2 further comprises ciphering the biometrics data and transmitting said  
3 transaction request message containing the ciphered biometrics data to said  
4 network, and wherein the step (d) further comprises the step of deciphering  
5 the biometrics data contained in the received authentication request message.

1 25. The identification method of claim 24, wherein the biometrics  
2 data contained in the transaction request message is ciphered by using a  
3 secret key which varies with time and agrees with the secret key with which  
4 the ciphered biometrics data is deciphered at said user authenticator.

1 26. An identification method comprising the steps of:  
2 a) transmitting, from an end terminal, a transaction request  
3 message containing biometrics data of a user to a communications network;  
4 b) receiving, at an electronic commerce service provider, said  
5 transaction request message via said network;  
6 c) transmitting, from said service provider, an authentication  
7 request message containing said biometrics data to said network;  
8 d) receiving, at a user authenticator having a database in which a  
9 plurality of registered biometrics data are mapped to a plurality of



10 corresponding registered user identifiers, said authentication request  
11 message via said network;  
12 e) comparing the received biometrics data to all of the registered  
13 biometrics data in said database to detect coincidence;  
14 f) detecting the user identifier mapped to the biometrics data  
15 which coincides with the received biometrics data; and  
16 g) returning a reply from the user authenticator to said service  
17 provider via said network indicating that said user having the detected user  
18 identifier is authenticated.

1 27. The identification method of claim 26, wherein the step (a)  
2 further comprises ciphering the biometrics data and transmitting said  
3 transaction request message containing the ciphered biometrics data to said  
4 network, and wherein the step (d) further comprises the step of deciphering  
5 the biometrics data contained in the received authentication request message.

1 28. An identification system comprising:  
2 a plurality of end terminals, each of the end terminals transmitting to a  
3 communications network a registration request message and a transaction  
4 request message, each of said messages containing biometrics data of a user  
5 and a user identifier of said user;  
6 at least one electronic commerce service provider (ECSP) unit for  
7 receiving said registration request message via said network to retransmitting  
8 the registration request message to said network and receiving said  
9 transaction request message via said network and transmitting an

10 authentication request message containing said biometrics data and said user  
11 identifier to said network; and  
12 an authentication server for receiving said registration request  
13 message from said ECSP unit via said network, mapping in a database a  
14 plurality of biometrics data contained in a plurality of said registration  
15 request messages to a plurality of corresponding user identifiers contained in  
16 said registration request messages, the authentication server further receiving  
17 the authentication request message via said network, comparing the received  
18 biometrics data to one of the biometrics data which is mapped in said  
19 database to the user identifier contained in said authentication request  
20 message and returning a reply to said ECSP unit via said network indicating  
21 that said transaction request message is authenticated if the received  
22 biometrics data coincides with said mapped biometrics data.

1 29. An identification system comprising:  
2 a plurality of end terminals, each of the end terminals transmitting a  
3 registration request message containing biometrics data of a user and a user  
4 identifier of the user to a communications network and transmitting a  
5 transaction request message containing said biometrics data to the  
6 communications network;  
7 at least one electronic commerce service provider (ECSP) unit for  
8 receiving said registration request message via said network and  
9 retransmitting the registration request message to said network and receiving  
10 said transaction request message and transmitting an authentication request  
11 message containing said biometrics data to said network; and

12 an authentication server for receiving said registration request  
13 message from said ECSP unit via said network, mapping a plurality of  
14 biometrics data contained in a plurality of said registration request messages  
15 to a plurality of corresponding user identifiers contained in said registration  
16 request messages, the authentication server receiving the authentication  
17 request message via said network, comparing the received biometrics data to  
18 all of the biometrics data in said database, detecting the user identifier  
19 mapped to the biometrics data which coincides with the received biometrics  
20 data, and returning a reply to said ECSP unit via said network indicating that  
21 a user identified by the detected user identifier is authenticated.

0934560-034560